Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-27. (canceled)

28. (new) A method of cloaking encrypted data, comprising:

encapsulating a serial data stream of encrypted data into IP packets;

forming a first tunnel for an overall IP link;

forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

transmitting said IP packets of encrypted data on a public IP network.

29. (new) The method of cloaking encrypted data according to claim 28, wherein:

said public network is an Internet.

30. (new) The method of cloaking encrypted data according to claim 28, wherein:

said IP packets are transmitted via an ISDN router.

31. (new) The method of cloaking encrypted data according to claim 28, wherein:

said IP packets are transmitted over a satellite terminal.

32. (new) The method of cloaking encrypted data according to claim 28, further comprising:

encrypting data using a Type 1 encryption unit.

33. (new) The method of cloaking encrypted data according to claim 32, wherein said Type 1 encryption unit comprises:

a KIV type encryption unit.

34. (new) The method of cloaking encrypted data according to claim 33, wherein said Type 1 KIV-type encryption unit comprises:

a KIV-7 encryption unit.

35. (new) The method of cloaking encrypted data according to claim 28, wherein said serial data stream of encrypted data comprises:

Voice over IP (VoIP) data.

36. (new) The method of cloaking encrypted data according to claim 28, wherein:

said serial data stream is a synchronous serial data stream.

37. (new) The method of cloaking encrypted data according to claim 36, wherein:

said synchronous serial data stream is an RS-530 data stream.

38. (new) The method of cloaking encrypted data according to claim 28, further comprising:

combining data from two voice sources into said serial data stream before said encapsulation.

39. (new) Apparatus for cloaking encrypted data in a deployable, secure communication terminal, comprising:

means for encapsulating a serial data stream of encrypted data into IP packets;

means for forming a first tunnel for an overall IP link; and

means for forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

means for transmitting said IP packets of encrypted data on a public IP network.

40. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein:

said public network is an Internet.

41. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein:

said IP packets are transmitted via an ISDN router.

42. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein:

said IP packets are transmitted over a satellite terminal.

43. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, further comprising:

means for encrypting data using a Type 1 encryption unit.

44. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein said Type 1 encryption unit comprises:

a KIV type encryption unit.

45. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 44, wherein said Type 1 KIV-type encryption unit comprises:

a KIV-7 encryption unit.

46. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein said serial data stream of encrypted data comprises:

Voice over IP (VoIP) data.

47. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein:

said serial data stream is a synchronous serial data stream.

48. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 47, wherein:

said synchronous serial data stream is an RS-530 data stream.

49. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, further comprising:

means for combining data from two voice sources into said serial data stream before said means for encapsulating encapsulates said serial data stream.

50. (new) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 49, wherein said means for combining data from two voice sources comprises:

a voice-enabled router.

51. (new) A secure communications device, comprising:

means for encrypting a data stream into an encrypted data stream;

means for encapsulating said encrypted data stream for transmission to another secure communications device using IP protocol; and

means for forming a first tunnel for an overall IP link; and

means for forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

means for routing said encapsulated, encrypted data stream over an Internet.

52. (new) The secure communications device according to claim 51, wherein said means for routing comprises:

an Ethernet to ISDN router.

53. (new) The secure communications device according to claim 51, wherein said means for encrypting comprises:

A KIV-7 encryption unit.

54. (new) The secure communications device according to claim 51, wherein:

said means for encapsulating converts a RS-530 synchronous serial data stream into an IP data stream.